ERICSSON

Date: July 31, 2026

Ericsson AB
Group Function Technology
SE-164 80 Stockholm
SWEDEN

Comments on ECCG Agreed Cryptographic Mechanisms 3.0

Dear ENISA and European Cybersecurity Certification Group,

Please find below Ericsson's detailed comments on ECCG ACM 3.0.

General comments on the use of ACM:

– We think ACM is a good document for the purpose it was designed for: Common Criteria-based cybersecurity certification. Our primary concern is the emerging tendency to use ACM as an allowlist for cryptographic mechanisms. This would have severe negative implications for innovation, security, and the long-term economic competitiveness of Europe.

  There is an important distinction between certification requirements and technology governance. For certification purposes, it is reasonable and necessary to define a stable set of cryptographic mechanisms that evaluators can assess against. Certification requires predictability, consistency, and clearly defined evaluation criteria. However, using the same document as a general allowlist for all cryptographic mechanisms would turn a certification tool into a technology gatekeeping mechanism. New cryptographic mechanisms often emerge from academic research, open competition, and industrial development many years before they become mature enough for formal approval processes.

  An allowlist creates significant barriers for innovation. In practice, a cryptographic allowlist would risk severely limiting European cryptographic innovation across all areas of cryptography, including anonymous credentials, digital wallets, zero-knowledge proofs, homomorphic encryption, secure multi-party computation, and threshold cryptography. This is particularly concerning because many of Europe's strategic digital initiatives depend on continued innovation in privacy-preserving cryptography. The European Commission has emphasized privacy, data minimization, and user control as core principles for the European Digital Identity Wallet, highlighting capabilities such as selective disclosure that allow users to prove information while revealing only the minimum necessary data. These capabilities rely on advanced cryptographic techniques, including zero-knowledge proofs and related privacy-enhancing mechanisms.

  Preventing European organizations from deploying new privacy-focused cryptography would not only harm innovation but would also significantly reduce the security and privacy protection available to European citizens and organizations. Privacy-enhancing cryptography is not merely a research topic; it is increasingly becoming a critical security

technology for protecting identities, reducing unnecessary disclosure of personal data, and improving resilience against large-scale data breaches and surveillance.

European industry cannot be expected to make substantial long-term investments in cryptographic R&D if new cryptographic mechanisms may have to wait many years for possible approval by the ECCG before they can be deployed. This creates significant uncertainty that substantially discourages investment and innovation. European companies need to be able to use global standards and competitive technologies in order to compete internationally. This would also appear to conflict with the European Commission's stated objective of strengthening European innovation, competitiveness, and technological leadership. The Commission has repeatedly emphasized the importance of fostering innovation, supporting research and development, and ensuring that European companies can compete in global markets. A restrictive cryptographic allowlist risks creating the opposite effect by making it harder for European researchers and companies to develop and deploy new cryptographic technologies.

Any use of ACM as a cryptographic allowlist is incompatible with maintaining a competitive and innovative European cryptographic ecosystem. ACM is valuable as guidance for certification evaluations, but turning it into a general restriction on the use of cryptographic mechanisms would have consequences far beyond certification and risks undermining Europe's digital sovereignty, innovation, competitiveness, and cybersecurity.

- An increased focus on cryptographic algorithm lists is the wrong priority for European cybersecurity. Relatively few practical vulnerabilities stem from weaknesses in the cryptographic algorithms themselves. Far more serious vulnerabilities result from incorrect use of otherwise secure algorithms, such as failing to perform public-key validation, deriving keys from low-entropy passwords, or using fixed IVs. An even larger share of vulnerabilities arises from weaknesses in cryptographic protocols and implementation flaws, such as buffer overflows and other software bugs. There is already an excessive focus on cryptographic algorithm selection, leading many users to believe that the choice of algorithms is the primary determinant of security. Elevating the role of ACM in European cybersecurity risks reinforcing this misconception, potentially reducing rather than improving overall cybersecurity.

- We encourage the ECCG to adopt a level of transparency equal to, or greater than, that of US NIST. This includes organizing public workshops; removing references to paywalled cryptographic specifications; maintaining public, archived mailing lists for discussion; publishing pre-draft call for comments, as well as one or more Initial Public Drafts with sufficiently long public comment periods; and making all submitted comments publicly available. Public archives are particularly important not only for openness, but also for long-term traceability, enabling stakeholders to review how decisions were made and to clearly identify who proposed, supported, or challenged specific choices. This level of accountability is critical in cryptography, where concerns about hidden weaknesses or potential backdoors are frequently raised; transparent and attributable discussions help build confidence that specifications have undergone broad scrutiny and are free from undisclosed influence. Transparency and openness are essential for building trust in cybersecurity and cryptography. The Chinese Next-Generation Commercial Cryptographic Algorithms Program (NGCC) has committed to a comparable level of transparency as NIST. Europe risks undermining confidence in its cryptographic standardization efforts if it does not demonstrate at least the same degree of openness.

General comments on the document:

- We suggest assigning numbers to all tables, as this is a standard practice in document design and improves readability and referencing.

- We welcome practical considerations such as "Attacks requiring access to more than 2^{64} blocks of data are thus not of practical concern." We encourage including more such considerations, particularly regarding memory requirements, circuit depth, and the number of online forgery attempts.

- "it will be revised on a two-year basis"

  Based on the current state of the document and the rapid pace of developments in cryptography and cryptanalysis, we believe that the proposed revision frequency is insufficient. We suggest that the document be reviewed and revised once per year.

- We suggest updating the document to align with the NIST post-quantum security levels 1–5 rather than using the outdated bits of security. In our view, these five quantum-resistance security levels should become the common reference framework for both symmetric and asymmetric cryptography in the future.

- The document references several withdrawn specifications. We consider withdrawn cryptographic specifications a security risk. We suggest that ACM removes all references to withdrawn specifications.

- The document references several paywalled specifications. Paywalled cryptographic specifications are increasingly seen as unacceptable cybersecurity risks. It becomes difficult to verify whether some parties selectively receive weakened versions. Paywalled standards also receive far less scrutiny from security researchers, increasing the likelihood that vulnerabilities go unnoticed. Paywalls increase the risk of flawed implementations, and we have encountered implementations of XTS-AES that appear to have been implemented from Wikipedia, omitting essential security requirements. Paywalls also significantly hinder validation that implementations correctly follow security requirements, both within and across organizations. Both European and US courts have emphasized that specifications with legal effect must be accessible. Access to cryptographic specifications is increasingly recognized as a human right. NIST and IETF has removed many references to paywalled standards and indicated that it will continue to do so. Our understanding is also that future Chinese NGCC algorithms will be freely available. Against this background, we strongly suggest that ACM removes all references to paywalled cryptographic specifications.

Comments on Section 2 (Symmetric Atomic Primitives)

Comments on Section 2.1 (Block Ciphers):

- *"In symmetric cryptography, the security is based on the confidentiality of a key shared by the legitimate users."*

  This should be revised to "confidentiality, integrity, and authenticity of a key", aligning with the text in Section 8. The integrity and authenticity of symmetric keys are critical and are a frequent source of vulnerabilities caused by implementation and operational errors. A common misconception among developers and users is that keys require only confidentiality. If an attacker can replace a key with one of their choosing, they can both decrypt and forge protected messages. If an attacker can modify bits in a key, they may induce two-time-pad scenarios or enable related-key attacks. With 2^r related keys an attacker can find all the 2^r keys with time complexity $\approx 2^{k-r}$. The same comment applies to Section 3.

- The AES specification reference [FIPS197] was withdrawn in 2023 and superseded by [FIPS197-upd1]. The maintained specification includes clarifications, corrections, improved descriptions of the key schedules, and expanded discussion of implementation considerations, including side-channel attacks. Relying on withdrawn or superseded cryptographic specifications is not state-of-the-art and introduces the risk of implementing outdated or corrected-out behavior, including ambiguities resolved in later revisions, and may lead to non-interoperable or insecure implementations. We recommend replacing all references to [FIPS197] with [FIPS197-upd1].

- The DES specification reference [FIPS46-3] was withdrawn in 2005 and superseded by [SP800-67], which itself was withdrawn in 2024. NIST now permits Triple-DES only for decryption, key unwrapping, and MAC verification of already protected data. We recommend replacing all references to [FIPS46-3] with [SP800-67] and adding a note that the specification has been withdrawn.

- While Advanced Encryption Standard remains widely trusted from a cryptanalytic perspective, secure implementation is non-trivial. In particular, high-performance software implementations without dedicated hardware support are notoriously difficult to implement in a fully constant-time manner. Implementations based on lookup tables or other secret-dependent memory accesses are typically vulnerable to timing and cache side-channel attacks capable of recovering secret key material. Implementers should therefore use dedicated cryptographic instructions, such as AES-NI, ARMv8 Cryptography Extensions, RISC-V cryptographic extensions, or equivalent hardware-assisted constant-time implementations. We suggest adding a note highlighting these AES implementation considerations.

- Triple-DES is not an atomic primitive according to the definition in Section 1.2, since its underlying component, single DES, is seen in practice. We suggest removing the term "atomic" from the document entirely and avoiding a distinction between atomic and non-atomic primitives. The theoretical discussion of atomic versus non-atomic primitives does not add value to the document.

- The idea that symmetric cryptography will be practically affected by CRQCs is now seen as a misconception. While classical supercomputers might be able to brute force AES-128 around the year 2090, a huge cluster of one billion CRQCs (according to one estimate costing one billion USD each) would take a million years of uninterrupted calculation to find a single AES-128 key. Algorithms with quadratic (n^2) speedup like Grover's algorithm (which is proven to be optimal) will not provide any practical quantum advantage for breaking symmetric cryptography. Breaking a single AES-128 key would require qubits covering the surface area of the Moon, and brute-forcing a single 191-bit key would require qubits covering the surface area of the red supergiant star Betelgeuse. See [IETF, 3GPP, Moon] for further details. Replacing AES-128 and SHA-256 would cost hundreds of billions of euros while providing very limited security benefit. Spreading misconceptions about quantum threats risks undermining trust in the ACM document as a whole. We suggest that Notes 3, 4, 19, and 71 be removed from the document.

- We suggest adding the block size n to the Table in Section 2.1. The block size is a fundamental security parameter affecting the security of most block cipher modes.

- The narrow 128-bit block size of AES is a major limiting factor in most modes of operation. For example, if AES-256-GCM is used with 96-bit random nonces, the attack complexity is only $\approx 2^{96-r}$, for AES-256-CMAC the integrity advantage is bounded by $q^2/2^{128}$. Avoiding these limitations requires complex and hard to analyze beyond-birthday bound (BBB) constructions.
  In both cases, the 128-bit block size, rather than the key size, is the primary factor limiting security. We suggest adding a note highlighting that the narrow block size of AES constitutes a major security limitation in many modes of operation.

- We suggest that Rijndael-256, i.e., Rijndael with a 256-bit key and 256-bit block size, be added as an agreed and recommended block cipher primitive. Rijndael-256 was designed by European cryptographers, and has been standardized by 3GPP and ETSI SAGE for use in MILENAGE-256 [TS35.235]. NIST is also planning to standardize Rijndael-256 for use in the Acc256 and wGCM constructions.

Comments on Section 2.2 (Stream Ciphers):

- *"A synchronous binary stream cipher allows to encrypt a plaintext of arbitrary length L bits by deriving a binary L-bit keystream sequence from a k-bit key and an n-bit initialization value and bitwise combining modulo 2 the plaintext sequence and the keystream sequence. The obtained L-bit sequence represents the ciphertext."*

  This describes a specific non-authenticated encryption construction based on a stream cipher primitive. Just like block ciphers, streams ciphers are flexible primitives that can be used also for integrity and authenticated encryption such as AEADs. We suggest changing the definition of stream cipher primitives to:

  "A synchronous stream cipher is a keyed algorithm that, given a secret k-bit key and an n-bit initialization value (IV) or nonce, generates a pseudorandom keystream of arbitrary length L. This keystream can be combined with data in different ways depending on the cryptographic construction."

- AES is currently the only recommended encryption primitive in ACM, and once Triple-DES is deprecated in 2027 it will become the sole remaining agreed primitive. This leads to a single-primitive landscape, which reduces cryptographic agility. Cryptographic agility is a fundamental security principle: systems should be able to replace cryptographic primitives without major redesign if a primitive is weakened or broken. In hardware deployments, this is typically achieved by supporting multiple independently designed primitives, enabling algorithm migration and diversity. It has long been a design principle in 3GPP and ETSI SAGE to mandate at least two diverse cryptographic algorithms to avoid single points of failure. We therefore suggest that ECCG considers adding additional agreed primitives based on different cryptographic constructions.

- We suggest that the stream cipher primitives SNOW 3G [SNOW3G], SNOW 5G [TS35.240], and ChaCha20 [RFC8439] are added as agreed and recommended stream cipher primitives. These algorithms were designed by European industrial and academic cryptographers and have been standardized by 3GPP/ETSI SAGE and the IETF CFRG, respectively.

  SNOW 3G uses a 128-bit key and forms the basis for the 3GPP confidentiality and integrity algorithms GEA5, GIA5, UEA2, UIA2, EEA1, EIA2, NEA1, and NIA1. It has been widely deployed and supported across 2G, 3G, 4G, and 5G systems, and is primarily optimized for efficient hardware implementation, while also remaining viable in software environments.

  SNOW 5G uses a 256-bit key and represents an evolution of the SNOW design, offering improved performance and a higher security margin. It forms the basis for the 5G algorithms NEA4, NIA4, and NCA4, and is expected to be optional in current 5G deployments but mandatory to support in future 6G security architectures. NCA4 (SNOW 5G in GCM-SST mode) achieves performance comparable to AES-GCM on modern CPUs, and can significantly outperform AES-GCM in hardware implementations, making it well suited to both software and hardware optimized environments.

  ChaCha20 uses a 256-bit key and is standardized in [RFC8439]. It is widely deployed in Internet protocols such as TLS and QUIC and has become a de facto standard in modern secure communications. ChaCha20 is designed for efficient and constant-time software implementation, particularly on platforms without AES hardware acceleration, where secure and timing-attack-resistant AES implementations are more difficult to achieve. As such, it is primarily optimized for software environments and provides a robust alternative to AES-based constructions.

Comments on Section 2.3 (Hash Functions) and 2.4 (XOF):

- We believe TurboSHAKE128, TurboSHAKE256, KT128, and KT256 [RFC9861] should be added as agreed algorithms.
- We believe the TupleHash128, TupleHash256, ParallelHash128, ParallelHash256 [SP800-185] should be added as agreed algorithms.

- We believe Ascon-Xof, Ascon-CXOF128, and Ascon-Hash256 [SP800-232] should be added as agreed algorithms.

- We believe that SHA-2 should have a note explaining that it is not indifferentiable from a random oracle due to structural properties such as length-extension and multicollision attacks. This was the cause of the weaknesses in SPHINCS+. In our view, NIST made the

wrong decision by allowing SHA-2 as an option for SLH-DSA, resulting in a significantly more complex specification than necessary. As part of the migration to post-quantum cryptography, SHA-2 should be phased out in favor of modern hash functions such as SHA-3/SHAKE.

Comments on Other Sections

- We welcome that ECCG uses the term "cryptographic protocol", it is important that developers and users understand that protocols are equally much cryptography as algorithms.

- *"Transport Layer Security (TLS) [RFC5246, RFC8446], formerly also known as Secure Socket Layer (SSL), is a protocol to protect the communication over the Internet, e.g. connection via HTTP (HTTPS)."*

  We suggest removing "over the Internet". TLS is used for a vast amount of non-Internet use cases including data centers, enterprise networks, internal device communication between processes and components, and HTTPS is used in 5G core networks [TS33.501].

  Note that HTTPS is an informal term that is not used in modern RFCs, which uses the more precise terms "https URI scheme" and "HTTP/2 over TLS". Note that HTTP/3 and HTTP/2 over TLS profiles TLS and comes with additional security requirements. The document should not talk about HTTP without mentioning HTTP/3, which uses QUIC.

- *"a common set of cryptographic mechanisms, the ciphersuite"*

  This is not correct, the cipher suite in TLS 1.3 only determines the AEAD and the KDF, the rest of the cryptographic mechanisms (key exchange mechanisms and signature algorithms) are negotiated in the Supported Groups, Key Share, Signature Algorithms, Signature Algorithms Certificate, and PSK Key Exchange Modes extensions. Modern TLS 1.2 works similarly.

- *The result of the execution of this protocol is a set of session data.*

  We find this is vague and slightly misleading terminology. We suggest "The result is a set of cryptographic parameters and shared secrets (session state)"

- While TLS 1.3 can be used with minimal profiling, a profile is still recommended. TLS 1.2 requires strict profiling to be considered even admissible. The ACM TLS profile is far from state-of-the-art and is very problematic for security aware companies and industries. Some companies go recommendation shopping and will continue to sell weak products as long as they can find any government that does not forbid use.

- *"In order to avoid protocol downgrade attacks, SSLv2 must not be supported."*

  This gives the impression that it is acceptable to support SSL 3.0, TLS 1.0, and TLS 1.1, which should not be the case. US government states that these obsolete versions of TLS gives false sense of security [NSA-TLS] and 3GPP has forbidden support since many years [TS33.210].

- *"It is recommended to use a ciphersuite offering perfect forward secrecy"*

  We believe this should be a strict requirement. US Pentagon is e.g. forbidding use of all symmetric key exchange [Pentagon].

- As Section 6 is very outdated and only covers TLS, we recommend completely removing Section 6.

- *"In this document, we limit ourselves to considering password and PIN-based person authentication solutions"*

  That seems contrary to the state of the art. These methods should not be used without multi-factor authentication. Furthermore, the described solutions have a significant impact on availability, which is the third and often overlooked component of the CIA information security triad.

- *"The use of encryption schemes supposes a communication between two parties"*

  File and disk encryption is typically used by a single party.

- *"The direct use of a pure true random generator is not agreed."*

  This is a very important topic, not only because of the risks posed by weak random number generators, but also because of the possibility of attacker-controlled physical randomness sources. We recommend following the Pentagon's lead and completely prohibiting the use of quantum key distribution (QKD) and non-local quantum randomness generation [Pentagon].
  In addition to the high risk that some QKD and QRNG vendors may be owned or controlled by foreign intelligence agencies, we are aware of at least one commercial QKD products that simply transmit classically generated random numbers between the communicating parties.

- *"In case the primality test does not prove the primality of the tested number, the probability that this number is composite should be lower that 2^{-125}"*

  We believe the probability should be connected to the security level of the generated key. A probability of 2^{-125} is fine for RSA-3072, but not for higher security levels such as RSA-8192. For probabilistic attacks, the time complexity is typically calculated as the amount of work divided by the success probability. We recommend adding a note to all RSA algorithms that supporting large keys may enable denial-of-service attacks.

- *"The management of keys by the product should not enable a potential attacker to recover any information about secret and private keys used to protect user information, nor to alter or inject public keys used to protect identities.*

  We suggest changing to

  "The management of keys by the product should not enable a potential attacker to recover any information about secret and private keys, nor to alter or inject secret, private, and public keys.

- *"private part can be generated locally and needs to be protected for confidentiality at all costs"*

Protecting the integrity of private keys is equally important. An attacker injecting its own private key can decrypt information or falsely claim to have signed information.

- *"A key established through key establishment should not be used directly but first postprocessed by an agreed key derivation function"*

  For key establishments where this is required, the output should not be referred to as a key, but rather as a shared secret. The text should clarify that, in modern key establishment algorithms, such as ML-KEM, key derivation is performed internally by the algorithm. Using a KDF to derive an n-bit output key from an n-bit input key without any additional entropy as input marginally decreases entropy.

- *"or a master secret in the case of the generation of TLS"*

  TLS has renamed this value to the master secret to align with inclusive language guidelines.

- "A key must not be used with different mechanisms"

  We believe there should be an exception for use within a single protocol, provided that the security of such use has been formally analyzed and proven, see e.g., [Thormarker].

- *"The distribution of secret and private keys shall be limited to the trusted environment that makes an effective use of the key."*

  This should include storage, backup, and in many enterprise and government use cases, key escrow.

- *"In the context of Diffie-Hellman key establishment schemes, these ephemeral keys"*

  Should remove "Diffie-Hellman" as the text is true for ephemeral KEM and PKE keys as well.

- We believe Ascon-AEAD128 [SP 800-232] should be added as an agreed algorithm.

- Appendix B specifies RSA key generation; however, it is underspecified and introduces non-standard constraints that do not align with either [RFC8017] or [FIPS186-5]. Including detailed algorithm specifications appears to be out of scope compared with the rest of the document. We suggest removing Appendix B and instead adding a note in Section 4.1 that specifies any additional requirements beyond those defined in [RFC8017] or [FIPS186-5].

- We strongly suggest that Appendix C adds a requirement that non-withdrawn and freely available specifications are mandatory for inclusion in ACM. Ericsson considers such specifications to be a security risk. We have removed all paywalled cryptographic specifications from our internal guidelines and are opposed to their normative use in any SDO.

- We do not believe that ACM should recommend SecP256r1MLKEM768 and SecP384r1MLKEM1024. The primary design goal for these hybrid schemes is to enable vendors to market FIPS-validated implementations of P-256 and P-384 as "quantum-resistant," even though only the quantum-vulnerable classical components are FIPS-certified. We consider this practice highly questionable and not something ACM should

encourage. Furthermore, these hybrids are unnecessary, as X25519MLKEM768 provides better performance, stronger practical robustness, and universal support across TLS libraries. As part of the migration to post-quantum cryptography, NIST P-curves and other Weierstraß curves should be phased out in favor of modern widely supported alternatives such as Curve25519 and Curve448.

- We suggest adding a note to CasKDF explaining that some of the options allowed in [ETSI] do not provide IND-CCA security. We believe that a requirement for hybrid constructions should be that they do not reduce the security properties the components.

- Note 53 states that ML-DSA should not be used standalone. While ACM refers to established standards for KEM combiners, it does not refer to any standard for hybrid signatures. We suggest clarifying that the approach: "For digital signatures, hybridization can consist of concatenating signatures from different schemes, with the verification function accepting if and only if all signatures are valid." is only acceptable for non-composite hybrids. When used to create composite signatures, this approach defines an entirely new signature algorithm that may significantly reduce the security properties of the component signatures. Examples include losing the beyond-unforgeability properties and introducing malleability vulnerabilities. The absence of such properties has resulted in severe practical vulnerabilities.

  We note that the Web ecosystem will use standalone ML-DSA. Widespread implementation and deployment are important security considerations that should be taken into account when selecting cryptographic schemes. We believe that the urgent migration of long-lived roots-of-trust to PQC is significantly more important for European cybersecurity than the choice between PQ/T hybrids and standalone post-quantum schemes.

John Preuß Mattsson,
Expert Cryptographic Algorithms and Security Protocols
MSc Business Administration and Economy

References

[3GPP] 3GPP Statement on PQC Migration
https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_118_Hyderabad/docs/S3-244307.zip

[FIPS186-5] Digital Signature Standard (DSS)
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf

[FIPS197-upd1] Advanced Encryption Standard (AES)
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf

[IETF] IETF Statement on Quantum Safe Cryptographic Protocol Inventory
https://datatracker.ietf.org/liaison/1942/

[Moon] Quantum Attacks on AES
https://www.youtube.com/watch?v=eB4po9Br1YY&t=3227s

[NSA-TLS] Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations
https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF

[Pentagon] Post Quantum Cryptography Strategy
https://dodcio.defense.gov/Portals/0/Documents/Library/DoW-PQC-Strategy.pdf

[RFC8017] PKCS #1: RSA Cryptography Specifications Version 2.2
https://www.rfc-editor.org/rfc/rfc8017.html

[RFC8439] ChaCha20 and Poly1305 for IETF Protocols
https://www.rfc-editor.org/rfc/rfc8439.html

[RFC9861] KangarooTwelve and TurboSHAKE
https://www.rfc-editor.org/rfc/rfc9861.html

[SNOW3G] SNOW 3G Algorithm Specification
https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2019/05/snow3gspec.pdf

[SP800-67] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-67r2.pdf

[SP800-232] Ascon-Based Lightweight Cryptography Standards for Constrained Devices
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-232.pdf

[Thormarker] On using the same key pair for Ed25519 and an X25519 based KEM
https://eprint.iacr.org/2021/509.pdf

[TS33.210] Network Domain Security (NDS); IP network layer security
https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279

[TS33.501] Security architecture and procedures for 5G System
https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

[TS35.235] Specification of the MILENAGE-256 algorithm
https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4244

[TS35.240] Specification of the Snow 5G based 256-bits algorithm set
https://www.3gpp.org/ftp/Specs/archive/35_series/35.240/35240-k00.zip